# Linear Threshold Multisecret Sharing Schemes*

Oriol Farràs, Ignacio Gracia, Sebastià Martín and Carles Padró
{ofarras,ignacio,sebasm,cpadro}@ma4.upc.edu

Dept. Matemàtica Aplicada IV, Universitat Politècnica de Catalunya (UPC), Barcelona, Spain

**Abstract.** In a multisecret sharing scheme, several secret values are distributed among a set of $n$ users, and each secret may have a different associated access structure. We consider here unconditionally secure schemes with multithreshold access structures. Namely, for every subset $P$ of $k$ users there is a secret key that can only be computed when at least $t$ of them put together their secret information. Coalitions with at most $w$ users with less than $t$ of them in $P$ cannot obtain any information about the secret associated to $P$. The main parameters to optimize are the length of the shares and the amount of random bits that are needed to set up the distribution of shares, both in relation to the length of the secret. In this paper, we provide lower bounds on this parameters. Moreover, we present an optimal construction for $t = 2$ and $k = 3$, and a construction that is valid for all $w$, $t$, $k$ and $n$. The models presented use linear algebraic techniques.

**Key words:** unconditional security, multisecret sharing schemes, threshold access structures.

## 1 Introduction

### 1.1 Multisecret Sharing Schemes

In a secret sharing scheme some secret information is distributed into shares among a set of users in such a way that only authorized coalitions of users can reconstruct the secret from their shares. Such a scheme is said to be perfect if unauthorized subsets of users do not obtain any information about the secret.

Multisecret sharing schemes are a generalization of such schemes. In a multisecret sharing scheme a number of secret values are distributed; we use $\mathcal{J}$ as the set of indices for this secret values. For each one of these secrets there will be some coalitions authorized to know it, and some other coalitions that will not be able to obtain any information about it.

For every $j \in \mathcal{J}$, we call $\Gamma_j$ the access structure associated with the secret corresponding to the index $j$, that is the collection of subsets authorized to

* This work was partially supported by the Spanish Ministry of Science and Technology under project TSI2006-02731.

know that particular secret. We also call $\Delta_j$ the forbidden structure associated with the secret corresponding to the index $j$, that is the collection of subsets unauthorized to know it. Naturally, the collection of subsets $\Gamma_j$ is monotone increasing, while $\Delta_j$ is monotone decreasing. Obviously, $\Gamma_j \cap \Delta_j = \emptyset$ for every $j \in \mathcal{J}$.

In a multisecret sharing scheme we define the *specification structure* $\Gamma$ as the collection of pairs of access and forbidden structures associated with the secret indexed by the elements in $\mathcal{J}$,
$\Gamma = \{(\Gamma_j, \Delta_j) : j \in \mathcal{J}\}$.

Multisecret sharing schemes are defined as a collection of random variables satisfying certain properties in terms of Shannon entropy. We denote by $S_i$ the random variable associated with the share of user $i \in \mathcal{U}$. Likewise, if $A = \{i_1, \ldots, i_r\}$ is a set of users, then $S_A$ is the random variable associated with the shares of users in $A$, that is $S_A = S_{i_1} \times \cdots \times S_{i_r}$.

A *perfect multisecret sharing scheme with specification structure* $\Gamma = \{(\Gamma_j, \Delta_j) : j \in \mathcal{J}\}$ is formed by two collections, $\{S_i\}_{i \in \mathcal{U}}$ and $\{K_j\}_{j \in \mathcal{J}}$, of random variables satisfying:

1. If $A \in \Gamma_j$ then $H(K_j|S_A) = 0$.
2. If $B \in \Delta_j$ then $H(K_j|S_B) = H(K_j)$.

The random variables $\{S_i\}_{i \in \mathcal{U}}$ correspond to the secret information distributed among the users, while the random variables $\{K_j\}_{j \in \mathcal{J}}$ correspond to the shared secret keys. Observe that, with this definition, we require the schemes to be unconditionally secure, namely the forbidden subsets cannot obtain any information on the secrets, independently of the computational power of the adversary.

The efficiency of a multisecret sharing scheme is measured by means of the complexity $\sigma$ and the randomness $\sigma_T$. The complexity $\sigma$ is the ratio between the amount of information received by every user and the amount of information corresponding to the key. The randomness $\sigma_T$ is the ratio between the amount of information distributed to the set of users $\mathcal{U}$ and the amount of information corresponding to the key. Namely,

$$\sigma = \frac{\max_{i \in \mathcal{U}} H(S_i)}{\min_{j \in \mathcal{J}} H(K_j)} \qquad \sigma_T = \frac{H(S_{\mathcal{U}})}{\min_{j \in \mathcal{J}} H(K_j)}$$

We observe that both complexity and randomness are greater or equal than 1. These parameters are a generalization of the ones used to measure the efficiency of secret sharing schemes. As for the easier case of secret sharing schemes, the optimization of these parameters for general specification structures is a very difficult open problem. Nevertheless, in the seminal paper on secret sharing by Shamir [10], optimal schemes are presented for threshold access structures. In contrast, no general optimal constructions of multisecret sharing schemes are known for this simple case of threshold specification structures. The optimality of such a construction is proved by comparing its complexity to some lower bound. General lower bounds for the complexity of multisecret sharing schemes with threshold structure were given in [7]. We present here general lower bounds

for the randomness of such schemes. Optimal constructions are only known for very particular values of the thresholds [1, 3, 8]. Shamir's polynomial construction of secret sharing schemes was generalized by Brickell [5] and Simmons [11], by using linear algebra technics; specifically they introduced linear secret sharing schemes. The same development took place in key predistribution schemes. The polynomial construction by Blundo et al. [3] was generalized by Padró et al. [9] to a linear construction. This linear framework is the starting point in our new approach to multithreshold schemes.

### 1.2 Multithreshold Sharing Schemes

This paper presents constructions of multisecret sharing schemes for some type of specification structures defined by thresholds. These kind of schemes are called multisecret threshold sharing schemes, or multithreshold schemes for short, and were introduced by Jackson, Martin and O'Keefe [7].

In these schemes, every secret is associated with a subset $P \subset \mathcal{U}$ of $k$ users. Shares distributed among users must be created in such a way that every subset with at least $t$ users in $P$ is authorized to know $P$'s secret, and every subset with at most $w$ users, having less than $t$ users in $P$, is unauthorized.

The specification structure of a multithreshold schemes depends on four positive integers $w$, $t$, $k$ and $n$ satisfying:

- $1 \leq t \leq k \leq n$
- $t - 1 \leq w \leq n - k + t - 1$

On a set $\mathcal{U}$ of $n$ users, the specification structure of a $w$-secure $(t, k, n)$ multithreshold sharing scheme is defined as follows:

- $\mathcal{J} = \{P \subseteq \mathcal{U} : |P| = k\}$
- For every $P \in \mathcal{J}$,
  - $\Gamma_P = \{A \subseteq \mathcal{U} : |A \cap P| \geq t\}$
  - $\Delta_P = \{B \subseteq \mathcal{U} : |B| \leq w, |B \cap P| \leq t - 1\}$

When $k = n$, then a single secret is shared. In this case, we have a threshold access structure, and the threshold sharing scheme by Shamir [10] provides an optimal solution. If $t = 1$, then we have a Key Predistribution Scheme (KPS). Optimal constructions were given in [3].

Complete $w$-secure $(t, k, n)$ multithreshold schemes are those with $w = n - k + t - 1$. If a multithreshold scheme is complete, for any $P \in \mathcal{J}$ and $B \subseteq \mathcal{U}$, a subset $B$ such that $|B \cap P| < t$ is $P$-unauthorized.

### 1.3 Known Results

The first multisecret schemes were multithreshold schemes with $t = 1$, and they were called Key Predistribution Schemes (KPS) [3]. In these schemes, any user in $P \in \mathcal{J}$ can calculate $P$'s secret by itself without any additional information. There are some interesting constructions of KPSs: the model presented in [3],

based on symmetric polynomials, and the model in [9], called Linear KPS, designed using linear maps. Linear KPS unify the previous proposals of KPS. On the other hand, when $k = n$ and $w = t - 1$, then we have a threshold secret sharing scheme [10].

In the rest of constructions of multithreshold schemes, $t = 2$. Namely, Jackson, Martin and O'Keefe found a geometric construction of an $(n-k+1)$-secure $(2, k, n)$ multithreshold scheme [8]. Moreover, Barwick and Jackson [1] gave another geometric construction for $w$-secure $(2, 3, n)$ multithreshold schemes.

Jackson, Martin and O'Keefe studied in [7] some bounds on the size of shares, and gave a lower bound on the complexity of a $w$-secure $(2, 3, n)$.

### 1.4 Our Results

We present here a new framework to study multisecret sharing schemes. We introduce the concept of linear multisecret sharing scheme that extends the corresponding notion in secret sharing and key predistribution schemes. This formal setting simplifies the security proofs in the constructions of multisecret sharing schemes.

By using our approach, we present a new construction of a $w$-secure $(2, 3, n)$ multithreshold scheme with optimal complexity and randomness that is simpler than the scheme with the same properties given by Barwick and Jackson [1].

We find a new lower bound on the randomness of a multithreshold scheme. Furthermore, by using entropies we present a new proof for the lower bound on the complexity given in [7].

Finally, in Section 5, we present a general construction of $w$-$(t, k, n)$ multithreshold scheme for general values of the parameters. In general, this is not an optimal scheme, but it is the best known construction that applies to all possible values of the parameters $w, t, k, n$.

## 2 Lower Bounds on the Complexity and Randomness

The complexity and the randomness of a scheme, defined in Section 1.2, are ratios that indicate the amount of information the trusted authority sends to users. This section is devoted to study the information rates of multithreshold schemes, namely to proof the next theorem, a result that provides bounds for the complexity and the randomness of multithreshold schemes.

**Theorem 1.** *Let $\mathcal{U} = \{1, \ldots, n\}$ be the set of users of a $w$-secure $(t, k, n)$ multithreshold scheme, such that $H(K_Q)$ is the same for every $Q \in \mathcal{J}$ and $H(S_i)$ is the same for every $i \in \mathcal{U}$. Then, we have following lower bounds on the complexity $\sigma$ and the randomness $\sigma_T$:*

$$\sigma \geq \binom{w+k-2t+1}{k-t} \qquad \sigma_T \geq \left(\binom{w+k-2t+2}{k-t+1} + (t-1)\binom{w+k-2t+1}{k-t}\right)$$

The following technical lemmas show properties of the entropy of keys in a multithreshold scheme. They will be used to prove Theorem 1.

**Lemma 1.** *Let $X$, $Y$, $Z$ be three random variables, $H(X)$ the entropy of the variable $X$ and $H(Y|Z)$ the entropy of $Y$ conditional on $Z$. If $H(Y|Z) = 0$, then $H(X|Y) \geq H(X|Z)$ and $H(Z) \geq H(Y)$.*

**Lemma 2.** *Let $\mathcal{U} = \{1, \ldots, n\}$ be the set of participants of a $w$-secure $(t, k, n)$ multithreshold scheme. Let $A \subseteq \mathcal{U}' \subseteq \mathcal{U}$ such that $|\mathcal{U}'| = w + k - (t-1)$ and $|A| = t - 1$. Let $\mathcal{A}$ be the following collection of subsets: $\mathcal{A} = \{Q \in \mathcal{J} \mid A \subseteq Q \subseteq \mathcal{U}'\} = \{Q_1, \ldots, Q_\mu\}$, where $\mu = \binom{w+k-2(t-1)}{k-(t-1)}$.*
*Then, $H(K_{Q_i} \mid K_{Q_1}, \ldots, K_{Q_{i-1}}, K_{Q_{i+1}}, \ldots K_{Q_\mu}) = H(K_{Q_i})$ for every $Q_i \in \mathcal{A}$. That is, the random variables $K_{Q_1}, \ldots, K_{Q_\mu}$ are independent.*

*Proof.* Let $Q_i \in \mathcal{A}$ and $C = (\mathcal{U}' \setminus Q_i) \cup A$. Observe that $C$ consists of $w$ users. Since $C \cap Q_i = A$, then $|C \cap Q_i| = t - 1$, and therefore $C$ is an unauthorized subset related to the key associated with $Q_i$. That is, $H(K_{Q_i} \mid S_C) = H(K_{Q_i})$.

On the other hand, $C \cap Q_j \supsetneq A$ for every $j \neq i$, hence $|C \cap Q_j| \geq t$. Then, $C$ is an authorized subset related to the key associated with $Q_j$, that is $H(K_{Q_j} \mid S_C) = 0$, for every $j \neq i$. Moreover, $H(K_{Q_1}, \ldots, K_{Q_{i-1}}, K_{Q_{i+1}}, \ldots, K_{Q_\mu} \mid S_C) = 0$.

Now, using Lemma 1, it follows that
$H(K_{Q_i} \mid K_{Q_1}, \ldots, K_{Q_{i-1}}, K_{Q_{i+1}}, \ldots, K_{Q_\mu}) \geq H(K_{Q_i} \mid S_C)$. Consequently,
$H(K_{Q_i} \mid K_{Q_1}, \ldots, K_{Q_{i-1}}, K_{Q_{i+1}}, \ldots, K_{Q_\mu}) = H(K_{Q_i})$, and therefore the random variables associated with the keys of subsets in $\mathcal{A}$ are independent.

**Lemma 3.** *Let $\mathcal{U} = \{1, \ldots, n\}$ be the set of participants of a $w$-secure $(t, k, n)$ multithreshold scheme. Let $B \subseteq \mathcal{U}' \subseteq \mathcal{U}$ such that $|\mathcal{U}'| = w + k - (t-1)$ and $|B| = t$. Consider the following collection of subsets of $\mathcal{U}$: $\mathcal{B} = \{Q \in \mathcal{J} \mid B \subseteq Q \subseteq \mathcal{U}'\} = \{Q_1, \ldots, Q_\nu\}$, where $\nu = \binom{w+k-(t-1)-t}{k-t} = \binom{w+k-2t+1}{k-t}$.*

*Then, $H(K_{Q_i} \mid K_{Q_1} \ldots K_{Q_i - 1}, K_{Q_i+1}, \ldots, K_{Q_\nu}) = H(K_{Q_i})$ for every $Q_i \in \mathcal{B}$, that is, the random variables $K_{Q_1}, \ldots, K_{Q_\nu}$ are independent.*

*Proof.* Let $A$ be a subset of $B$ such with $t - 1$ elements. If we define $\mathcal{A}$ as in Lemma 2, observe that $\mathcal{B} \subseteq \mathcal{A}$, thus the random variables $K_{Q_1}, \ldots, K_{Q_\nu}$ are independent.

**Lemma 4.** *Under the conditions and notation of the preceding two lemmas, $H(K_{\mathcal{B}} \mid S_A) = H(K_{\mathcal{B}})$ and $H(K_{\mathcal{A}} \mid S_B) = H(K_{\mathcal{A} \setminus \mathcal{B}})$, for any subset $A \subseteq B$.*

*Proof.* Suppose, without loss of generality, that $A = \{1, \ldots, t-1\}$ and $B = \{1, \ldots, t\}$. For every $Q_i \in \mathcal{A}$ we define $C_i = (\mathcal{U}' \setminus Q_i) \cup A$. Observe that, as seen during the proof of Lemma 2,

$$H(K_{Q_i} \mid S_{C_i}) = H(K_{Q_i}) \text{ and } H(K_{Q_j} \mid S_{C_i}) = 0 \text{ for every } j \neq i.$$

On the other hand, due to entropy properties,

$$H(K_{\mathcal{B}} \mid S_A) = \sum_{i=1}^{\nu} H(K_{Q_i} \mid S_A K_{Q_1} \ldots K_{Q_{i-1}}).$$

Since $A \subseteq C_i$, it follows that $H(K_{Q_i} \mid S_A K_{Q_1} \dots K_{Q_{i-1}}) \geq H(K_{Q_i} \mid S_{C_i} K_{Q_1} \dots K_{Q_{i-1}})$. Furthermore, since $H(K_{Q_1} \dots K_{Q_{i-1}} \mid S_{C_i}) = 0$, it follows, that

$$H(K_{Q_i} \mid S_{C_i} K_{Q_1} \dots K_{Q_{i-1}}) = H(K_{Q_i} \mid S_{C_i}) = H(K_{Q_i}).$$

Hence,

$$H(K_{\mathcal{B}}) \geq H(K_{\mathcal{B}} \mid S_A) \geq \sum_{i=1}^{\nu} H(K_{Q_i}) = H(K_{\mathcal{B}}),$$

which leads to $H(K_{\mathcal{B}} \mid S_A) = H(K_{\mathcal{B}})$.
Using again entropy properties, we obtain

$$H(K_{\mathcal{A}} \mid S_B) = \sum_{i=1}^{\mu} H(K_{Q_i} \mid S_B K_{Q_1} \dots K_{Q_{i-1}}).$$

For every $Q_i$ in $\mathcal{B}$ we have $H(K_{Q_i} \mid S_B K_{Q_1} \dots K_{Q_{i-1}}) = 0$, because $|Q_i \cap B| = t$. For every $Q_i$ in $\mathcal{A} \setminus \mathcal{B}$, we have that $B \subseteq C_i$, thus

$$H(K_{Q_i} \mid S_B K_{Q_1} \dots K_{Q_{i-1}}) \geq H(K_{Q_i} \mid S_{C_i} K_{Q_1} \dots K_{Q_{i-1}}) =$$

$$= H(K_{Q_i} \mid S_{C_i}) = H(K_{Q_i}).$$

Hence,

$$H(K_{\mathcal{A}} \mid S_B) = \sum_{i \in \mathcal{A} \setminus \mathcal{B}} H(K_{Q_i} \mid S_B K_{Q_1} \dots K_{Q_{i-1}}) = \sum_{i \in \mathcal{A} \setminus \mathcal{B}} H(K_{Q_i}) = H(K_{\mathcal{A} \setminus \mathcal{B}}).$$

Finally, we provide the proof of Theorem 1.

*Proof.* First, we prove the upper bound on $\sigma$. Let $B = \{1, \dots, t\}$, $A = \{1, \dots, t-1\}$ and $\mathcal{U}' \subset \mathcal{U}$ such that $B \subset \mathcal{U}'$ and $|\mathcal{U}'| = w+k-t+1$, and consider the collection of subsets $\mathcal{B} = \{Q \in \mathcal{J} \mid B \subseteq Q \subset \mathcal{U}'\} = \{Q_1, \dots, Q_\nu\}$, where $\nu = \binom{w+k-(t-1)-t}{k-t}$.

Lemma 3 ensures that the variables $K_{Q_1}, \dots, K_{Q_\nu}$ are independent, thus $H(K_{\mathcal{B}}) = \nu H(K)$. Now, for every $Q \in \mathcal{B}$ we know $|B \cap Q| = t$ and $|A \cap Q| = t-1$, hence $H(K_Q \mid S_t S_A) = 0$ and $H(K_Q \mid S_A) = H(K_Q)$. Consequently, $H(K_{\mathcal{B}} \mid S_t S_A) = 0$ and, by Lemma 4, $H(K_{\mathcal{B}} \mid S_A) = H(K_{\mathcal{B}})$. Lemma 1 leads to $H(S) = H(S_t) \geq H(K_{\mathcal{B}}) = \nu H(K)$, and the desired upper bound on $\sigma$ is obtained.

Let $\mathcal{A}$ be the structure associated with $A$, defined in Lemma 2. In order to find an upper bound on $\sigma_T$ we use $H(S_{\mathcal{U}}) = H(S_B) + H(S_{\mathcal{U}} \mid S_B)$. First, we are going to bound $H(S_B)$. Since $H(S_B) = \sum_{i=1}^{t} H(S_i \mid S_1 \dots ...S_{i-1})$, $H(K_{\mathcal{B}} \mid S_t S_A) = 0$ and $H(K_{\mathcal{B}} \mid S_A) = H(K_{\mathcal{B}})$, then it follows that $H(S_t \mid S_A) \geq H(K_{\mathcal{B}})$. Now, since $H(S_i) = H(S)$ for every $i$, then $H(S_i \mid S_1, \dots ...S_{i-1}) \geq H(S_t \mid S_A)$, and therefore $H(S_B) \geq t \cdot \nu H(K)$.

Now, we are going to bound $H(S_{\mathcal{U}} \mid S_B)$. Since $H(K_{\mathcal{A}} \mid S_{\mathcal{U}}) = 0$, we have $H(S_{\mathcal{U}} \mid S_B) \geq H(K_{\mathcal{A}} \mid S_B)$. Applying Lemma 4, it follows that $H(K_{\mathcal{A}} \mid S_B) = (\mu - \nu) H(K)$, thus $H(S_{\mathcal{U}}) \geq (\mu + (t-1)\nu) H(K)$, and the desired upper bound on $\sigma_T$ is obtained.

## 3 Linear Multisecret Sharing Schemes

A useful method to define secret sharing schemes is to consider some linear maps to define the share of each user and the keys in the scheme. Using this kind of maps, it will be easy to check whether a coalition can obtain a key through a linear combination of their shares. Furthermore, the use of linear techniques can simplify the construction of the scheme.

In linear multisecret schemes, there are some vector spaces over a finite field $\mathbb{K}$ called $E$, $E_i$ and $V_P$ for every $i \in \mathcal{U}$ and $P \in \mathcal{J}$. There is a surjective linear map $\phi_i : E \to E_i$ for every $i \in \mathcal{U}$ that generates the secret information (the share) of each user, and there is a surjective linear map $\pi_P : E \to V_P$ for every $P \in \mathcal{J}$. Choosing $x \in E$ uniformly at random, $\pi_P(x)$ is $P$'s secret and $\phi_i(x)$ is the secret information of the user $i$.

Next result shows a property of linear maps widely used within the security proofs for most of the schemes presented in this paper. This result is Lemma 3.1 in [9].

**Lemma 5.** *Let $E, E_0$ and $E_1$ be vector spaces over a finite field $\mathbb{K}$. Consider two linear mappings, $\phi_0 : E \to E_0$ and $\phi_1 : E \to E_1$, where $\phi_0$ and $\phi_1$ are surjective. Suppose that a vector $x \in E$ is chosen uniformly at random. Then,*

1. *the value of $x_0 = \phi_0(x)$ can be uniquely determined from $x_1 = \phi_1(x)$ if and only if $\ker \phi_1 \subset \ker \phi_0$.*
2. *the value of $x_1$ provides no information about the value of $x_0$ if and only if $\ker \phi_1 + \ker \phi_0 = E$.*

A Key Predistribution Scheme (KPS) is a method by which a trusted authority distributes secret information among a set of users in such a way that every user belonging to a set in a family of privileged subsets is able to compute a common key associated with that set. This kind of schemes can be seen as multisecret schemes where the minimal authorized sets are single users.

C. Padró, I. Gracia, S. Martín and P. Morillo present in [9] some KPSs defined trough linear maps, that they call Linear KPS (LKPS). That paper presents a method to generate schemes that base their security on linear algebra properties. Next theorem is a generalization of Theorem 3.2 in [9] for multisecret sharing schemes with a given specification structure $\Gamma$.

**Theorem 2.** *Let $\Gamma$ be a specification structure on the set of $n$ users $\mathcal{U} = \{1, \ldots, n\}$. Let $E$ and $E_i \neq \{0\}$, for every $i \in \{0, 1, \ldots, n\}$, be vector spaces over a finite field $\mathbb{K}$. Suppose there exist a surjective linear mapping $\phi_i : E \to E_i$ for every user $i \in \mathcal{U}$ and a surjective linear mapping $\pi_P : E \to E_0$ for every subset $P \in \mathcal{J}$ satisfying:*

1. *$\bigcap_{i \in A} \ker \phi_i \subset \ker \pi_P$ for any $A \in \Gamma_P$.*
2. *$\bigcap_{j \in F} \ker \phi_j + \ker \pi_P = E$ for any $F \in \Delta_P$.*

*Then there exists a linear multisecret sharing scheme with specification structure $\Gamma$ whose complexity and randomness are:*

$$\sigma = \frac{\max_{i\in\mathcal{U}} \dim E_i}{\dim E_0} \qquad \sigma_T = \frac{\dim E}{\dim E_0}$$

*Proof.* The theorem is proven analogously to theorem 3.2 in [9]. We construct a scheme where we assume that $E$, $E_i$, $E_0$, $\pi_P$ and $\phi_i$ are publicly known, for all $i \in \mathcal{U}$ and $P \in \mathcal{J}$. Given an element $x \in E$ randomly chosen, the secret of $P \in \mathcal{J}$ is $\pi_P(x)$ and the share of user $i$ is $\phi_i(x)$.

Let $A = \{i_1, \ldots, i_r\}$ be a subset of users. We consider $\phi_A$ a map from $E$ to $E_{i_1} \times \cdots \times E_{i_r}$ defined as $\phi_A = \phi_{i_1} \times \ldots \times \phi_{i_r}$. Observe that $\phi_A(x)$ is the secret information known by the users of $A$ and, as $\phi_i$ is surjective for all $i \in \mathcal{U}$, $\phi_A$ is surjective for all $A \subset \mathcal{U}$.

Let $\Gamma_P$ and $\Delta_P$ be the collection of authorized and unauthorized subsets for a given $P$ in $\mathcal{J}$. If $A$ is in $\Gamma_P$, Lemma 5 says that $\pi_P(x)$ can be obtained from $\phi_A(x)$ if and only if $\ker \phi_A \subset \ker \pi_P$. But $\ker \phi_A = \bigcap_{i\in A} \ker \phi_i$, so by hypothesis this property holds. But if $F \in \Delta_P$, by hypothesis $\bigcap_{i\in F} \ker \phi_i + \ker \pi_P = E$, so it implies that $\ker \phi_F + \ker \pi_P = E$. By Lemma 5, users in $F$ cannot obtain any information about $\pi_P$, and the proof is concluded.

Observe that condition 1 in Theorem 2 guarantees $H(K_P \mid S_A) = 0$, so subsets in $\Gamma_P$ can calculate $P$'s secret. Besides, if the scheme satisfies condition 2, then we can ensure that $H(K_P \mid S_F) = H(K_P)$ for all subset in $\Delta_P$, so the scheme is perfect.

We will use Theorem 2 to construct our schemes, so we will use the same kind of operators and notation used in [9]. For all schemes presented in this paper, the keys are in $\mathbb{K}$, $E_0 = V_P = \mathbb{K}$ for all $P \in \mathcal{J}$.

## 4 An Optimal $w$-Secure $(2, 3, n)$ Multithreshold Scheme

In this section we present an optimal $w$-secure $(2, 3, n)$ multithreshold scheme constructed using linear techniques, according to the model discussed in section 3. In section 1.2 we have seen that $w$ must be an integer between 0 and $n-k+t-1$, so in our case $0 \leq w \leq n-2$. When $w = n-2$, this scheme is complete and allows a simpler model, which is presented in subsection 4.3.

In a $w$-secure $(2, 3, n)$ multithreshold scheme every subset of three users has a common secret, that will only be revealed if at least two of them share their secret information. If a subset $P \in \mathcal{J}$ has a secret, coalitions of $w$ users or less will have zero knowledge about $P$'s secret if such coalitions have at most one user in $P$. Considering the notation in 1.2, our case leads to:

- $|\mathcal{U}| = n$
- $\mathcal{J} = \{P \subseteq \mathcal{U} : |P| = 3\}$
- For all $P \in \mathcal{J}$,
  - $\Gamma_P = \{A \subseteq \mathcal{U} : |A \cap P| \geq 2\}$
  - $\Delta_P = \{B \subseteq \mathcal{U} : |B| \leq w, |B \cap P| \leq 1\}$

### 4.1 Optimal $w$-Secure $(2, 3, n)$ Multithreshold Scheme Construction

To design a linear multithreshold scheme, some vector spaces $E, E_0, E_1, \ldots, E_n$, defined over a finite field $\mathbb{K}$ are required. There is no restriction on the characteristic of $\mathbb{K}$ but, as we will see in subsection 4.2, the field must be large enough. The understanding of the scheme requires familiarity with linear algebra concepts such as dual vector space and tensor product. The appendix provides some notions on these subjects.

The trusted authority creates an identifier $x_i \in \mathbb{K} - \{0\}$ for each user $i \in \mathcal{U}$, that is public; let $X = \{x_i\}_{i\in\mathcal{U}}$. Then, the trusted authority privately sends to each user a linear map that depends on its identifier.

In the scheme presented in this section,

- $E = S_2(\mathbb{K}^w) \times (\mathbb{K}^w)^*$
- $E_i = (\mathbb{K}^w)^*$ for all $i \in \mathcal{U}$
- $E_0 = \mathbb{K}$
- For every $i \in \mathcal{U}$, the map $\phi_i : S_2(\mathbb{K}^w) \times (\mathbb{K}^w)^* \longrightarrow (\mathbb{K}^w)^*$ is defined as follows:
$$\phi_i(T, S) = T(v_i, \cdot) + \lambda_i S$$
- For every $P = \{i, j, k\} \in \mathcal{J}$, the map $\pi_P : S_2(\mathbb{K}^w) \times (\mathbb{K}^w)^* \longrightarrow \mathbb{K}$ is defined as follows:
$\pi_P(T, S) =$
$$= x_i{\cdot}\phi_i(T,S)(\lambda_k v_j - \lambda_j v_k) + x_j{\cdot}\phi_j(T,S)(\lambda_i v_k - \lambda_k v_i) + x_k{\cdot}\phi_k(T,S)(\lambda_j v_i - \lambda_i v_j)$$

where

- $\lambda_i = -x_i^w$ for all $i \in \mathcal{U}$
- $v_i = (1, x_i, x_i^2, \ldots, x_i^{w-1})$ for all $i \in \mathcal{U}$

The trusted authority chooses some $(T, S) \in S_2(\mathbb{K}^w) \times (\mathbb{K}^w)^*$ and distributes privately the linear forms $\phi_i(T, S)$ to every user in $\mathcal{U}$. This linear form is the secret information of each user. Given $P = \{i, j, k\}$ a subset in $\mathcal{J}$, if two users $i$ and $j$ share their secrets, using linearity of $S$ together with the symmetry and bilinearity of $T$, they can calculate $\pi_P(T, S)$. Namely, since for any $\{i, j, k\}{\subset}\mathcal{U}$ we have

$$[\phi_i(T,S)](\lambda_k v_j - \lambda_j v_k) + [\phi_j(T,S)](\lambda_i v_k - \lambda_k v_i) + [\phi_k(T,S)](\lambda_j v_i - \lambda_i v_j) = 0 \quad (1)$$

then,

$$\begin{aligned}\pi_P(T,S) = {} & x_i\phi_i(T,S)(\lambda_k v_j - \lambda_j v_k) + x_j\phi_j(T,S)(\lambda_i v_k - \lambda_k v_i) + \\ & + x_k(-\phi_i(T,S)(\lambda_k v_j - \lambda_j v_k) - \phi_j(T,S)(\lambda_i v_k - \lambda_k v_i)).\end{aligned}$$

For the sake of security in our constructions, in some cases $X$ needs to fulfill a condition. For a clearer formulation of this condition, we are going to introduce the following rational functions:

• $f(\mathbf{z}, y) = \sum_{i=1}^{w} z_i^w \cdot \prod_{j=1, j\neq i}^{w} \frac{y - z_j}{z_i - z_j}$,
where $y \in \mathbb{K}$, $\mathbf{z} = (z_1, \cdots, z_w) \in \mathbb{K}^w$, such that $z_i \neq z_j$ if $i \neq j$.

Observe that $f(\mathbf{z}, z_i) = z_i^w$, for every $i \in \{1, \cdots, w\}$.

• $g(\mathbf{z}, z_{w+1}, z_{w+2}, z_{w+3}) =$
$= (z_{w+1} - z_{w+2})[z_{w+3}^w f(\mathbf{z}, z_{w+1}) f(\mathbf{z}, z_{w+2}) + z_{w+1}^w z_{w+2}^w f(\mathbf{z}, z_{w+3})] +$
$+ (z_{w+2} - z_{w+3})[z_{w+1}^w f(\mathbf{z}, z_{w+2}) f(\mathbf{z}, z_{w+3}) + z_{w+2}^w z_{w+3}^w f(\mathbf{z}, z_{w+1})] +$
$+ (z_{w+3} - z_{w+1})[z_{w+2}^w f(\mathbf{z}, z_{w+3}) f(\mathbf{z}, z_{w+1}) + z_{w+3}^w z_{w+1}^w f(\mathbf{z}, z_{w+2})]$,

where $z_{w+1}, z_{w+2}, z_{w+3} \in \mathbb{K}$, $\mathbf{z} = (z_1, \cdots, z_w) \in \mathbb{K}^w$, such that $z_i \neq z_j$ if $i \neq j$.

Observe that $g(x_{i_1}, \ldots, x_{i_{w+3}})$ is well defined for every $(x_{i_1}, \ldots, x_{i_{w+3}}) \in X^{w+3}$. The condition on $X$ is:

**Condition 1.** $g(x_{i_1}, \ldots, x_{i_{w+3}}) \neq 0$ for every $(x_{i_1}, \ldots, x_{i_{w+3}}) \in X^{w+3}$.

Since the least common multiple of the denominators involved in the expression of $g$ is

$$m(\mathbf{z}) = \prod_{1 \leq i < j \leq w} (z_i - z_j)^2$$

then we will require that the polynomial

$$p(\mathbf{z}, z_{w+1}, z_{w+2}, z_{w+3}) = g(\mathbf{z}, z_{w+1}, z_{w+2}, z_{w+3}) \cdot m(\mathbf{z})$$

does not vanish for every $(x_{i_1}, \ldots, x_{i_{w+3}}) \in X^{w+3}$, for $x_{i_j} \neq x_{i_k}$ for $j \neq k$, and this implies a restriction on the size of the field $\mathbb{K}$. Namely, observe that the degree of every numerator in $f$ is $2w - 1$, and so the degree of every numerator in $g$ is at most $w + 1 + 2(2w - 1) = 5w - 1$. Consequently, $\deg(p) \leq (5w - 1) + 2[w(w - 1)]$.

Due to the symmetries in the definition of $f$ and $g$, it suffices to check that $p(\mathbf{z}, z_{w+1}, z_{w+2}, z_{w+3}) \neq 0$ only for $\binom{n}{3}\binom{n-3}{w}$ points in $X^{w+3}$. Therefore, applying Schwartz's Lemma (Theorem 6 in the appendix), the restriction on the size of the field is $|\mathbb{K}| > \binom{n}{3}\binom{n-3}{w}[2(5w - 1)w(w - 1)] + 1$.

Eventually, Condition 1 must be checked only once, at the beginning of the protocol. As we will see in 4.3, this condition will not be necessary when the scheme is complete.

### 4.2 Security Proof

**Theorem 3.** *Under Condition 1, the scheme just defined is an optimal $w$-secure $(2, 3, n)$ multithreshold scheme.*

*Proof.* In order to prove that this construction defines a $w$-secure $(2,3,n)$ multithreshold scheme we will use Theorem 2. Taking into account that the structure $\Delta_P$ is monotone decreasing and the structure $\Gamma_P$ is monotone increasing for all $P \in \mathcal{J}$, it is enough to prove the conditions in Theorem 2 for minimal subsets in $\Gamma_P$ and maximal subsets in $\Delta_P$. So we have to show that for any $P = \{i,j,k\} \in \mathcal{J}$ and for any subset of $P$ with two elements, e.g. $\{i,j\}$, then $\ker\phi_i \cap \ker\phi_j$ is included in $\ker\pi_P$, and for any $B \in \Delta_P$, with $|B| = w$, then $E = \bigcap_{i\in B} \ker\phi_i + \ker\pi_P$.

Suppose $(T,S)$ belongs to $\ker\phi_i \cap \ker\phi_j$ for some $i,j \in B$. Then, for every $\{i,j,k\} \in \mathcal{J}$, it follows from (1) that $[\phi_k(T,S)](\lambda_j v_i - \lambda_i v_j) = 0$. Now, if we calculate $\pi_P(T,S)$ for any $(T,S) \in \ker\phi_i \cap \ker\phi_j$ we see that $\pi_P(T,S) = 0$, so the first part is proved.

Now we have to prove the second part. Since $\pi_P$ is a linear map and the image of $\pi_P$ is $\mathbb{K}$, then $\dim\ker\pi_P = \dim E - 1$. Therefore it suffices to show that, for every $B \in \Delta_P$, there exists an element belonging to $\bigcap_{i\in B}\ker\phi_i$ that does not belong to $\ker\pi_P$.

As previously mentioned, it suffices to prove the second part for maximal subsets in $\Delta_P$, namely the subsets $B \in \Delta_P$ such that $|B| = w$. Observe that, given $P \in \mathcal{J}$ from a $w$-secure $(2,3,n)$ multithreshold scheme, $0 \le |B \cap P| \le 1$ for any $B \in \Delta_P$. Thus, given $P \in \mathcal{J}$ we will separately prove the condition for the cases $|B \cap P| = 0$ and $|B \cap P| = 1$.

First, we consider maximal subsets in $\Delta_P$ with one element in $P$. In order to simplify notation, we can assume, without loss of generality, that $P = \{1,2,3\}$ and $B = \{3,4,\ldots,w+2\}$. Clearly, $\{v_3, v_4, \ldots, v_{w+2}\}$ is a basis of $\mathbb{K}^w$, since $x_i \neq x_j$ for $i \neq j$.

Consider the operator $S \in (\mathbb{K}^w)^*$ such that $S(v_i) = -\lambda_i$ for all $i \in B$ and the operator $T = S \otimes S$. Observe that $T$ is a bilinear symmetrical operator, $T \in S_2(\mathbb{K}^w)$ (see Appendix A for more details). For any $i \in B$, $\phi_i(T,S) = (S\otimes S)(v_i,\cdot) + \lambda_i S = (S(v_i) + \lambda_i)S = 0$, thus $(T,S)$ belongs to $\bigcap_{i\in B}\ker\phi_i$. In particular, since $\{3\} = P \cap B$, the chosen operator satisfies $\phi_3(T,S) = 0$ and $S(v_3) = -\lambda_3$. Thus, it is straightforward to check that $\pi_P(T,S) = (x_1 - x_2)\lambda_3(S(v_1)+\lambda_1)(S(v_2)+\lambda_2)$.

Now, we check that $\pi_P(T,S) \neq 0$ showing that each factor is nonzero. By definition of $x_i$ and $\lambda_i$, $(x_1 - x_2)$ and $\lambda_3$ are different from zero. Let $p(x)$ be the polynomial of degree $w-1$ defined by $p(x) = S(1,x,\ldots,x^{w-1})$. Observe that $p(x_i) = x_i^w$ for all $i \in B = \{3,\ldots,w+2\}$. Suppose that $p(x)$ satisfies $p(x_2) = x_2^w$ (analogously for $p(x_1) = x_1^w$). Then $x^w - p(x)$ is a polynomial of degree $w$ with $w+1$ zeroes, which is a contradiction. Therefore, the result is proved for the maximal subsets in $\Delta_P$ having one element in common with $P$.

Now suppose $B$ and $P$ are disjoint and, without loss of generality, that $P = \{1,2,3\}$ and $B = \{4,\ldots,w+3\}$. Let $S$ be the operator defined by $S(v_i) = -\lambda_i$ for all $i \in B$ and $T = S \otimes S \in S_2(\mathbb{K}^w)$. Analogously to the other case, $(T,S)$ belongs to $\bigcap_{i\in B}\ker\phi_i$.

Let $p(x)$ be a polynomial defined, as above, by $p(x) = S(1,x,\ldots,x^{w-1})$. Since $p(x_i) = x_i^w$ for all $i \in B = \{4,\ldots,w+3\}$, by Lagrange interpolation, the

expression of this polynomial is

$$p(x) = \sum_{i=4}^{w+3} x_i^w \cdot \prod_{j=4, j\neq i}^{w+3} \frac{x - x_j}{x_i - x_j} = f(x, x_4, \ldots, x_{w+3})$$

If we express $\pi_P(T, S)$ replacing $S(v_i)$ by $p(x_i)$, we have

$$\begin{aligned}\pi_P(T,S) &= (x_1 - x_2)(\lambda_3 p(x_1)p(x_2) - \lambda_1\lambda_2 p(x_3)) \\ &+(x_2 - x_3)(\lambda_1 p(x_2)p(x_3) - \lambda_2\lambda_3 p(x_1)) \\ &+(x_3 - x_1)(\lambda_2 p(x_3)p(x_1) - \lambda_1\lambda_3 p(x_2)) = g(x_1, \ldots, x_{w+3})\end{aligned}$$

Taking into account condition 1, we can conclude that $\pi_P(T, S) \neq 0$. Hence, for all $B \in \Delta_P$, $\bigcap_{i\in B} \ker \phi_i + \ker \pi_P = E$, and the security proof is completed.

This scheme is optimal, so complexity and randomness obtained are minimum for a $w$-secure $(2, 3, n)$ multithreshold scheme.

Since $\dim(E_i) = \dim(\mathbb{K}^w)^* = w$ for all $i \in \mathcal{U}$ and $\dim E = \dim S_2(\mathbb{K}^w) + \dim(\mathbb{K}^w)^* = \binom{w+1}{2} + w$, then

$$\sigma = w \qquad \sigma_T = \tfrac{w(w+1)}{2} + w$$

According to Theorem 1, our scheme is optimal.

### 4.3 Optimal $(n-2)$- Secure $(2, 3, n)$ Multithreshold Scheme Construction

If the above scheme is complete, then $w = n - 2$, and Condition 1 is not needed to obtain an $(n - 2)$- secure $(2, 3, n)$ multithreshold scheme. The field $\mathbb{K}$ needs only to satisfy $|\mathbb{K}| > n$.

**Theorem 4.** *The scheme defined in subsection 4.1 is an optimal* $(n-2)$*- secure* $(2, 3, n)$ *multithreshold scheme.*

*Proof.* Observe that, in a $(n - 2)$- secure $(2, 3, n)$ multithreshold scheme, given $P \in \mathcal{J}$, if $B$ is a maximal subset in $\Delta_P$, since $|B| = n - 2$ then necessarily $|B \cap P| = 1$. For this reason, in this case, Condition 1 is not needed in the proof of Theorem 3.

## 5 $w$-Secure $(t, k, n)$ Multithreshold Scheme

In this section, we will design a family of $w$-secure $(t, k, n)$ multithreshold schemes for any possible values of $w$, $t$, $k$, $n$. Namely, $1 \leq t \leq k \leq n$ and $0 \leq w \leq n-k+t-1$, as seen in section 1.2. Unfortunately, these schemes are not optimal in general.

We also show how to design linear $w$-secure $(t, k', n)$ multithreshold schemes, for any $k'$ such that $t \leq k' < k$, from a given linear $w$-secure $(t, k, n)$ multithreshold.

Observe that for $t = 1$ this is an optimal linear KPS, and when $k = n$ and $w = t - 1$ the scheme presented is also optimal, since it is an ideal secret sharing scheme.

### 5.1 $w$-Secure $(t, k, n)$ Multithreshold Scheme Construction

Taking into account the definition of linear multithreshold schemes, we are going to define the vector spaces $E$ and $E_i$, for $i \in \{0, \ldots, n\}$, over a finite field $\mathbb{K}$. There is no restriction on the characteristic of $\mathbb{K}$, but the size of this field must be greater than $n$. Again, the understanding of the scheme requires some linear algebra concepts as dual vector space and tensor product (see Appendix A). During the setup phase, the trusted authority chooses $X = \{x_i\}_{i \in \mathcal{U}} \subseteq \mathbb{K} \setminus \{0\}$, such that $x_i \neq x_j$ if $i \neq j$, which will be the identifiers of users in $\mathcal{U}$.

Let $m = w - t + 2$. For the scheme presented in this section,

- $E = (S_k(\mathbb{K}^m))^t = S_k(\mathbb{K}^m) \times \overset{t)}{\cdots} \times S_k(\mathbb{K}^m)$
- $E_i = S_{k-1}(\mathbb{K}^m)$ for all $i \in \mathcal{U}$
- $E_0 = \mathbb{K}$

- For every $i \in \mathcal{U}$, the map $\phi_i : (S_k(\mathbb{K}^m))^t \longrightarrow S_{k-1}(\mathbb{K}^m)$ is defined as follows:

$$\phi_i(T_1, \ldots, T_t) = \lambda_{i,1} T_1(v_i, \ldots) + \cdots + \lambda_{i,t} T_t(v_i, \ldots)$$

  where
  - $v_i = (1, x_i, x_i^2, \ldots, x_i^{m-1}) \in \mathbb{K}^m$ for all $i \in \mathcal{U}$.
  - $\lambda_{i,j} = x_i^{j-1}$ for all $i \in \mathcal{U}$, $1 \leq j \leq t$.
- For every $P = \{i_1, \ldots, i_k\} \in \mathcal{J}$, the map $\pi_P : (S_k(\mathbb{K}^m))^t \longrightarrow \mathbb{K}$ is defined as follows:

$$\pi_P(T_1, \ldots, T_t) = T_1(v_{i_1}, \ldots, v_{i_k})$$

Let $P$ be a set in $\mathcal{J}$, and $A$ a subset of $t$ users in $P$. Without loss of generality, we can suppose that $P = \{1, \ldots, k\}$ and $A = \{1, \ldots, t\}$. Since $T_j$ is symmetrical, $T_j(v_i, v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_k) = T_j(v_1, \ldots, v_k)$, then user $i$ can calculate

$$s_{i,P} = \lambda_{i,1} T_1(v_1, \ldots, v_k) + \cdots + \lambda_{i,t} T_t(v_1, \ldots, v_k)$$

By sharing the values $s_{i,P}$, for $i = 1, \ldots, t$, the users in $A$ can solve the linear system

$$\begin{pmatrix} 1 & x_1 & \ldots & x_1^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & \ldots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} T_1(v_1, \ldots, v_k) \\ \vdots \\ T_t(v_1, \ldots, v_k) \end{pmatrix} = \begin{pmatrix} s_{1,P} \\ \vdots \\ s_{t,P} \end{pmatrix}$$

and they obtain the secret $T_1(v_1, \ldots, v_k)$.

The complexity and randomness of this scheme are:

$$\sigma = \tbinom{w+k-t}{k-1} \qquad \sigma_T = \tfrac{1}{t} \cdot \tbinom{w+k-t+1}{k}$$

Now we prove the validity of the scheme.

**Theorem 5.** *The scheme above defined is a $w$-secure $(t,k,n)$ multithreshold scheme.*

*Proof.* We follow the same steps as in the proof of Theorem 3. That is, it suffices to show that for any $P \in \mathcal{J}$, then every $A \subseteq P$ such that $|A| = t$ satisfies $\bigcap_{i\in A} \ker \phi_i \subseteq \ker \pi_P$, and every $B \in \Delta_P$ such that $|B| = w$, satisfies $\bigcap_{i\in B} \ker \phi_i + \ker \pi_P = E$.

Let $P = \{1,\ldots,k\} \in \mathcal{J}$ and $A = \{1,\ldots,t\} \subset P$. If we take $(T_1,\ldots,T_t)$ in $\bigcap_{i=1}^{t} \ker \phi_i$, then $\lambda_{i,1}T_1(v_i,\ldots) + \cdots + \lambda_{i,t}T_t(v_i,\ldots) = 0 \in S_{k-1}(\mathbb{K}^m)$ for every $i \in A$, and consequently $\lambda_{i,1}T_1(v_1,\ldots,v_k) + \cdots + \lambda_{i,t}T_t(v_1,\ldots,v_k) = 0$ for every $i \in A$.

Since $\lambda_{i,j} = x_i^{j-1}$, the above equations can be expressed as follows:

$$\begin{pmatrix} 1 & x_1 & \ldots & x_1^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & \ldots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} T_1(v_1,\ldots,v_k) \\ \vdots \\ T_t(v_1,\ldots,v_k) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Since $\left(x_i^{j-1}\right)_{i,j}$ is an invertible matrix, then $T_i(v_1,\ldots,v_k) = 0$, for every $i = 1,\ldots,t$. In particular, $T_1(v_1,\ldots,v_k) = 0$, and so $(T_1,\ldots,T_t) \in \ker \pi_P$.

Since $\pi_P$ is a non-zero linear form, then $\dim \ker \pi_P = \dim E - \dim \mathrm{Im}(\pi_P) = \dim E - 1$. Thus, to prove that for any $B \in \Delta_P$ we have $\bigcap_{i\in B} \ker \phi_i + \ker \pi_P = E$, it suffices to show that there exists an element belonging to $\bigcap_{i\in B} \ker \phi_i$ that does not belong to $\ker \pi_P$.

Let $B$ a maximal subset in $\Delta_P$, $F \subseteq B \setminus P$ such that $|F| = w - t + 1 = m - 1$, and $G$ the vector subspace of $\mathbb{K}^m$ with dimension $m-1$ spanned by $\langle v_i \rangle_{i\in F}$. Observe that, if $i \notin F$, then $v_i \notin G$. Let $\{e_1,\ldots,e_{m-1}\}$ be an orthogonal basis of $G$. Then, there exists a vector $e_m \in \mathbb{K}^m$ such that $\{e_1,\ldots,e_m\}$ is an orthogonal basis of $\mathbb{K}^m$. Let $(\mathbb{K}^m)^*$ be the dual space of $\mathbb{K}^m$ and $\{e^1,\ldots,e^m\}$ its dual basis. Now, consider the symmetric operator $\widehat{T} = e^m \otimes \overset{k)}{\cdots} \otimes e^m \in S_k(\mathbb{K}^m)$. It is straightforward to check that $\widehat{T}(v_i,\ldots) = 0$ for every $i \in F$, and $\widehat{T}(v_1,\ldots,v_k) \neq 0$, for $P = \{1,\ldots,k\}$.

Let $T = (\mu_1\widehat{T},\ldots,\mu_t\widehat{T}) \in (S_k(\mathbb{K}^m))^t$. We want to determine the coefficients $\mu_1,\ldots,\mu_t \in \mathbb{K}$ such that $T \in \bigcap_{i\in B} \ker \phi_i$, but $T \notin \ker \pi_P$. By definition of $\widehat{T}$, $\phi_i(T) = 0$ for every $i \in F$. On the other hand, $\phi_i(T) = \phi_i(\mu_1\widehat{T},\ldots,\mu_t\widehat{T}) = (\lambda_{i,1}\mu_1 + \cdots + \lambda_{i,t}\mu_t)\,\widehat{T}(v_i,\ldots)$, for every $i \in B \setminus F$. The homogeneous $(t-1)\times t$ linear system $\lambda_{i,1}\mu_1 + \cdots + \lambda_{i,t}\mu_t = 0$, where $i \in B \setminus F$ has non-trivial solution, and $\mu_i \neq 0$ for every $i \in B$ (if any $\mu_i$ were 0, then the resulting homogeneous $(t-1)\times(t-1)$ linear system would have only the trivial solution, $\mu_j = 0$ for every $j$).

Hence, we have found an operator $T$ in $\bigcap_{i\in B} \ker \phi_i$ such that $\pi_P(T) = \mu_1\widehat{T}(v_1,\ldots,v_k)$ is different from zero, so $T$ does not belong to $\ker \pi_P$. Therefore, the proof is completed.

### 5.2 A family of $w$-Secure $(t, k', n)$ Multithreshold Schemes, from a given $w$-Secure $(t, k, n)$ Multithreshold Scheme

As a final observation, we show how to construct, from a given $w$-secure $(t, k, n)$ multithreshold scheme, a $w$-secure $(t, k', n)$ multithreshold scheme for any $k'$ satisfying $t \leq k' < k$.

The new scheme is like the one in subsection 5.1, except for the following differences:

- The collection of subsets of users that have a key is $\mathcal{J}' = \{P' \subseteq \mathcal{U} : |P'| = k'\}$.
- To implement this scheme the set of users must be ordered, and this order must be known by every user.
- For every ordered set $P' = \{i_1, \ldots, i_{k'}\} \in \mathcal{J}'$, the map $\pi_P : (S_k(\mathbb{K}^m))^t \longrightarrow \mathbb{K}$ is defined as follows:

$$\pi_{P'}(T_1, \ldots, T_t) = T_1(v_{i_1}, \ldots, v_{i_{k'-1}}, v_{i_{k'}}, \ldots, v_{i_{k'}})$$

Let $P'$ be a set in $\mathcal{J}'$, and $A$ a subset of $t$ users in $P'$. Without loss of generality, we can suppose that $P' = \{1, \ldots, k'\}$ and $A = \{1, \ldots, t\}$. Since $T_j$ is symmetrical, then user $i$ can calculate

$$s_{i,P'} = \lambda_{i,1} T_1(v_1, \ldots, v_{k'-1}, v_{k'}, \ldots, v_{k'}) + \cdots + \lambda_{i,t} T_t(v_1, \ldots, v_{k'-1}, v_{k'}, \ldots, v_{k'})$$

Users from $A$ can share $s_{i,P'}$, $i = 1, \ldots, t$, and consequently they obtain the secret $T_1(v_1, \ldots, v_{k'-1}, v_{k'}, \ldots, v_{k'})$ associated with $P'$, by solving the following linear system:

$$\begin{pmatrix} 1 & x_1 & \ldots & x_1^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & \ldots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} T_1(v_1, \ldots, v_{k'-1}, v_{k'}, \ldots, v_{k'}) \\ \vdots \\ T_t(v_1, \ldots, v_{k'-1}, v_{k'}, \ldots, v_{k'}) \end{pmatrix} = \begin{pmatrix} s_{1,P'} \\ \vdots \\ s_{t,P'} \end{pmatrix}$$

## A Appendix

For the sake of completeness, this appendix contains some additional definitions and results. Since the schemes presented in this paper are based on linear maps and multilinear forms, we present here a brief introduction to the notions of dual space and multilinear forms over a vector space.

Given a vector space $E$ over a field $\mathbb{K}$, we define the *dual space* $E^*$ as the set of linear applications from $E$ to $\mathbb{K}$. The spaces $E$ and $E^*$ have the same dimension.

If $\{e_1, \ldots, e_n\}$ is a basis of $E$, then the *dual basis* $\{e^1, \ldots, e^n\}$ of $E^*$ is defined as follows:

$$e^i(e_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

Let $v = \sum_{i=1}^{n} \lambda_i e_i \in E$ and $w = \sum_{j=1}^{n} \mu_j e^j \in E^*$, then

$$w(v) = \sum_{j=1}^{n} \mu_j e^j (\sum_{i=1}^{n} \lambda_i e_i) = \sum_{i=1}^{n} \lambda_i \mu_i$$

Let $F$ be a subspace of $E$, then the *orthogonal subspace* of $F$ is the following subspace of $E^*$:

$$F^{\perp} = \{w \in E^* : w(v) = 0 \text{ for every } v \in F\}$$

A *multilinear form* in $E^n$ is a map from $E^n$ to $\mathbb{K}$ that is separately linear in each variable. If $w$ is a multilinear form in $E^n$, then $w = (w_1, \ldots, w_n) \in (E^*)^n$, and for every $v = (v_1, \ldots, v_n) \in E^n$ we have

$$\begin{aligned} w : E^n &\to \mathbb{K} \\ v &\mapsto w(v) = w_1(v_1)w_2(v_2)\cdots w_n(v_n) \end{aligned}$$

Multilinear forms that are invariant under permutation of its variables are called *symmetric multilinear forms*, and the subspace of symmetric multilinear forms in $E^n$ is $S_n(E)$. Observe that, given $w \in S_n(E)$, for every permutation $\sigma$ of $\{1, \ldots, n\}$ and for every $(v_1, \ldots, v_n) \in E^n$ we have:

$$w(v_1, \ldots, v_n) = w(v_{\sigma(1)}, \ldots, v_{\sigma(n)})$$

If $\dim E = m$, then $\dim S_n(E) = \binom{n+m-1}{n}$.

Finally, we provide Schwartz's Lemma.

**Theorem 6.** *(Schwartz's Lemma) Let $p \in \mathbb{K}[X_1, \ldots, X_N]$ be a nonzero polynomial on $N$ variables of degree $d < |\mathbb{K}|$. Then, there exists a point $(x_1, \ldots, x_N)$ in $\mathbb{K}^N$ such that $p(x_1, \ldots, x_N) \neq 0$.*

## References


1. S.G. Barwick, W.-A. Jackson. An Optimal Multisecret Threshold Scheme Construction. *Designs, Codes and Cryptography* Vol. 37 (2005) pp. 367-389.
2. G.R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings* 48 (1979) 313-317.
3. C. Blundo, A. DeSantis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung. Perfectly secure key distribution for dynamic conferences. *Advances in Cryptology- Crypto '92*, Lecture Notes in Computer Science, 740 (1993) 471-486.
4. C. Blundo, P. D'Arco, V. Daza, C. Padró. Bounds and constructions for unconditionally secure distributed key distribution schemes for general access structures. *Theoretical Computer Science*, 320 (2004) 269-291.
5. E.F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. and Combin. Comput.* **9** (1989) 105–113.
6. T.M. Cover, J.A. Thomas, Elements of Information Theory. *John Wiley & Sons*(1991).

7. W.-A. Jackson, K.M. Martin and C.M. O'Keefe. Multisecret threshold schemes. *Advances in Cryptology - Crypto '93*, Lecture Notes in Computer Science, 773 (1994) 126-135.
8. W.-A. Jackson, K.M. Martin and C.M. O'Keefe. A Construction for Multisecret Threshold Schemes. *Designs Codes Cryptography* 9 (1996) 287-303.
9. C. Padró, I. Gracia, S. Martín Molleví and P. Morillo. Linear Key Predistribution Schemes, *Designs, Codes and Cryptography* 25 (2002) 281-298.
10. A. Shamir. How to share a secret. *Commun. of the ACM.* 22 (1979) 612-613.
11. G. J. Simmons. How to (Really) Share a Secret. *Advances in Cryptology – CRYPTO '88, Lecture Notes in Comput. Sci.* **403** (1990) 390–448.
12. D.R. Stinson, On some methods for unconditionally secure key distribution and broadcast encryption.*Designs, Codes and Cryptography* Vol. 12 (1997) pp.215-243.